

Effective Differential Lüroth's Theorem*

Lisi D'Alfonso[‡]

Gabriela Jeronimo[‡]

Pablo Solernó[‡]

[‡] Departamento de Ciencias Exactas, Ciclo Básico Común, Universidad de Buenos Aires,
Ciudad Universitaria, 1428, Buenos Aires, Argentina

[‡] Departamento de Matemática and IMAS, UBA-CONICET,
Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires,
Ciudad Universitaria, 1428, Buenos Aires, Argentina

E-mail addresses: lisi@cbc.uba.ar, jeronimo@dm.uba.ar, psolerno@dm.uba.ar

February 29, 2012

Abstract

This paper focuses on effectivity aspects of the Lüroth's theorem in differential fields. Let \mathcal{F} be a differential field of characteristic 0 and $\mathcal{F}\langle u \rangle$ be the field of differential rational functions generated by a single indeterminate u . Let be given non constant rational functions $v_1, \dots, v_n \in \mathcal{F}\langle u \rangle$ generating a subfield $\mathcal{G} \subseteq \mathcal{F}\langle u \rangle$. The differential Lüroth's theorem proved by Ritt in 1932 states that there exists $v \in \mathcal{G}$ such that $\mathcal{G} = \mathcal{F}\langle v \rangle$. Here we prove that the total order and degree of a generator v are bounded by $\min_j \text{ord}(v_j)$ and $(nd(e+1)+1)^{2e+1}$, respectively, where $e := \max_j \text{ord}(v_j)$ and $d := \max_j \deg(v_j)$. We also present a new probabilistic algorithm which computes the generator v with controlled complexity.

1 Introduction

In 1876, J. Lüroth in [18] presented his famous result, currently known as the Lüroth's Theorem: if $k \subset L \subset k(u)$ is an extension of fields, where $k(u)$ is the field of rational functions in one variable u , then $L = k(v)$ for a suitable $v \in L$ (see [27, §10.2] for a modern proof). In 1893 G. Castelunovo solved the same problem for rational function fields in two variables over an algebraically closed ground field. For three variables, Lüroth's problem has been solved negatively.

In 1932 J.F. Ritt [22] addressed the differential version of this result: *Let \mathcal{F} be a differential field of characteristic 0, u an indeterminate over \mathcal{F} and $\mathcal{F}\langle u \rangle$ the smallest field containing \mathcal{F} , u and all its derivatives. Then, if \mathcal{G} is a differential field such that*

*Partially supported by the following Argentinian grants: ANPCyT PICT 2007/816, UBACYT 2002010010041801 (2011-2014) and UBACYT 20020090100069 (2010-2012)

$\mathcal{F} \subset \mathcal{G} \subset \mathcal{F}\langle u \rangle$, there is an element $v \in \mathcal{G}$ such that $\mathcal{G} = \mathcal{F}\langle v \rangle$. Such an element will be called a Lüroth generator of the extension $\mathcal{F} \subset \mathcal{G}$.

In fact, Ritt considered the case of differential fields \mathcal{F} of meromorphic functions in an open set of the complex plane being \mathcal{G} a finite extension of \mathcal{F} . Later E. Kolchin in [15] and [16] gave a new proof of this theorem for any differential field of characteristic 0 and without the hypothesis of finiteness on \mathcal{G} . Contrary to the classical setting, the differential Lüroth problem fails does not hold the case of two variables (see [21]).

The present paper deals with quantitative aspects of the Differential Lüroth's Theorem and the computation of a Lüroth generator v of a finite differential field extension. More precisely, let \mathcal{F} be a differential field of characteristic 0, u differentially transcendental over \mathcal{F} and $\mathcal{G} := \mathcal{F}\langle P_1(u)/Q_1(u), \dots, P_n(u)/Q_n(u) \rangle$, where $P_j, Q_j \in \mathcal{F}\{u\}$ are relatively prime differential polynomials of order at most $e \geq 1$ (i.e. at least one derivative of u occurs in P_j or Q_j for some j) and total degree bounded by d such that $P_j/Q_j \notin \mathcal{F}$ for every $1 \leq j \leq n$. First, we prove that any Lüroth generator v of $\mathcal{F} \subset \mathcal{G}$ can be written as the quotient of two relatively prime differential polynomials $M_1(u), M_2(u) \in \mathcal{F}\{u\}$ with order bounded by $\min\{\text{ord}(P_j/Q_j); 1 \leq j \leq n\}$ (see Proposition 11 below) and total degree bounded by $(nd(e+1) + 1)^{2e+1}$ (see Section 5.2).

Secondly, we exhibit a probabilistic procedure, called Algorithm **LurothGenerator** (see Theorem 16), which computes differential polynomials $M_1(u), M_2(u)$ such that its quotient is a Lüroth generator. If the input polynomials P_j, Q_j , $1 \leq j \leq n$, are given by a straight-line program of length L (for a definition and properties of straight-line programs see [2] and [13]), the number of arithmetic operations in \mathcal{F} performed by the algorithm is linear in L and polynomial in n, d, e and the degree of an algebraic variety \mathbb{V} associated to the input polynomials (see Notation 13 for the precise definition of \mathbb{V}).

An algorithmic version of Ritt's proof of the differential Lüroth's Theorem is given in [8] but no quantitative questions on the order or the degree of the Lüroth generator are addressed and no complexity analysis of the algorithm is performed (for effectiveness considerations of the classical not differential version, we refer the interested reader to [20], [25], [1], [9], [10], [3]).

Our approach combines elements of Ritt's and Kolchin's proofs (mainly the introduction of the differential polynomial ideal related to the graph of the rational map $u \mapsto (P_j/Q_j)_{1 \leq j \leq n}$) with estimations concerning the order and the differentiation index of differential ideals developed in [24], [4] and [5]. These estimations allow us to reduce the problem to a polynomial ring in finitely many variables. In this context, we are able to apply techniques of algorithmic resolution of algebraic polynomial systems *à la Kronecker* as in [5] and [6] (see [12] and [26]) in order to obtain a probabilistic procedure with controlled complexity which computes the Lüroth generator.

This paper is organized as follows. In Section 2 we introduce the notations, definitions and previous results from differential algebra (mainly concerning the order and the differentiation index) needed in the rest of the paper. In Section 3 we discuss some ingredients that appear in the classical proofs of Lüroth's Theorem by Ritt and Kolchin and that we will use in our arguments. In Section 4 and 5 we prove bounds for the order and

the degree, respectively, of any Lüroth generator. Section 6 is devoted to the algorithm and its complexity. Finally, in Section 7 we show how the algorithm works in two simple examples.

2 Preliminaries

In this section we introduce the notation used throughout the paper and recall some definitions and results from differential algebra.

2.1 Basic definitions and notation

A *differential field* (\mathcal{F}, δ) is a field \mathcal{F} equipped with a derivation $\delta : \mathcal{F} \rightarrow \mathcal{F}$; for instance, $\mathcal{F} = \mathbb{Q}, \mathbb{R}$ or \mathbb{C} with $\delta = 0$, or $\mathcal{F} = \mathbb{Q}(t)$ with the usual derivation $\delta(t) = 1$.

Let (\mathcal{F}, δ) be a differential field of characteristic 0.

The ring of differential polynomials in α indeterminates $z := z_1, \dots, z_\alpha$, which is denoted by $\mathcal{F}\{z_1, \dots, z_\alpha\}$ or simply $\mathcal{F}\{z\}$, is defined as the commutative polynomial ring $\mathcal{F}[z_j^{(p)}, 1 \leq j \leq \alpha, p \in \mathbb{N}_0]$ (in infinitely many indeterminates), extending the derivation of \mathcal{F} by letting $\delta(z_j^{(i)}) = z_j^{(i+1)}$, that is, $z_j^{(i)}$ stands for the i th derivative of z_j (as customarily, the first derivatives are also denoted by \dot{z}_j). We write $z^{(p)} := \{z_1^{(p)}, \dots, z_\alpha^{(p)}\}$ and $z^{[p]} := \{z^{(i)}, 0 \leq i \leq p\}$ for every $p \in \mathbb{N}_0$.

The fraction field of $\mathcal{F}\{z\}$ is a differential field, denoted by $\mathcal{F}\langle z \rangle$, with the derivation obtained by extending the derivation δ to the quotients in the usual way. For $g \in \mathcal{F}\{z\}$, the *order of g with respect to z_j* is $\text{ord}(g, z_j) := \max\{i \in \mathbb{N}_0 : z_j^{(i)} \text{ appears in } g\}$, and the *order of g* is $\text{ord}(g) := \max\{\text{ord}(g, z_j) : 1 \leq j \leq \alpha\}$; this notion of order extends naturally to $\mathcal{F}\langle z \rangle$ by taking the maximum of the orders of the numerator and the denominator in a reduced representation of the rational fraction.

Given a finite set of differential polynomials $H = h_1, \dots, h_\beta \in \mathcal{F}\{z\}$, we write $[H]$ to denote the smallest *differential ideal* of $\mathcal{F}\{z\}$ containing H (i.e. the smallest ideal containing the polynomials H and all their derivatives of arbitrary order). The minimum *radical differential ideal* of $\mathcal{F}\{z\}$ containing H is denoted by $\{H\}$. For every $i \in \mathbb{N}$, we write $H^{(i)} := h_1^{(i)}, \dots, h_\beta^{(i)}$ and $H^{[i]} := H, H^{(1)}, \dots, H^{(i)}$.

A *differential field extension* \mathcal{G}/\mathcal{F} consists of two differential fields $(\mathcal{F}, \delta_{\mathcal{F}})$ and $(\mathcal{G}, \delta_{\mathcal{G}})$ such that $\mathcal{F} \subseteq \mathcal{G}$ and $\delta_{\mathcal{F}}$ is the restriction to \mathcal{F} of $\delta_{\mathcal{G}}$. Given a subset $\Sigma \subset \mathcal{G}$, $\mathcal{F}\langle \Sigma \rangle$ denotes the minimal differential subfield of \mathcal{G} containing \mathcal{F} and Σ .

An element $\xi \in \mathcal{G}$ is said to be *differentially transcendental* over \mathcal{F} if the family of its derivatives $\{\xi^{(p)} : p \in \mathbb{N}_0\}$ is algebraically independent over \mathcal{F} ; otherwise, it is said to be *differentially algebraic* over \mathcal{F} . A *differential transcendence basis* of \mathcal{G}/\mathcal{F} is a minimal subset $\Sigma \subset \mathcal{G}$ such that the differential field extension $\mathcal{G}/\mathcal{F}\langle \Sigma \rangle$ is differentially algebraic. All the differential transcendence bases of a differential field extension have the same cardinality (see [14, Ch. II, Sec. 9, Theorem 4]), which is called its *differential transcendence degree*.

2.2 Differential polynomials, ideals and manifolds

Here we recall some definitions and properties concerning differential polynomials and their solutions.

Let $g \in \mathcal{F}\{z\} = \mathcal{F}\{z_1, \dots, z_\alpha\}$. The *class* of g for the order $z_1 < z_2 < \dots < z_\alpha$ of the variables is defined to be the greatest j such that $z_j^{(i)}$ appears in g for some $i \geq 0$ if $g \notin \mathcal{F}$, and 0 if $g \in \mathcal{F}$. If g is of class $j > 0$ and of order p in z_j , the *separant* of g , which will be denoted by S_g , is $\partial g / \partial z_j^{(p)}$ and the *initial* of g , denoted by I_g , is the coefficient of the highest power of $z_j^{(p)}$ in g .

Given g_1 and g_2 in $\mathcal{F}\{z\}$, g_2 is said to be of *higher rank in z_j than g_1* if either $\text{ord}(g_2, z_j) > \text{ord}(g_1, z_j)$ or $\text{ord}(g_2, z_j) = \text{ord}(g_1, z_j) = p$ and the degree of g_2 in $z_j^{(p)}$ is greater than the degree of g_1 in $z_j^{(p)}$. Finally, g_2 is said to be of *higher rank than g_1* if g_2 is of higher class than g_1 or they are of the same class $j > 0$ and g_2 is of higher rank in z_j than g_1 .

We will use some elementary facts of the well-known theory of *characteristic sets*. For the definitions and basic properties of rankings and characteristic sets, we refer the reader to [14, Ch. I, §8-10].

Let H be a (not necessarily finite) system of differential polynomials in $\mathcal{F}\{z\}$. The *manifold of H* is the set of all the zeros $\eta \in \mathcal{G}^\alpha$ of H for all possible differential extensions \mathcal{G}/\mathcal{F} .

Every radical differential ideal $\{H\}$ of $\mathcal{F}\{z\}$ has a unique representation as a finite irredundant intersection of prime differential ideals, which are called the *essential prime divisors* of $\{H\}$ (see [23, Ch. II, §16-17]).

For a differential polynomial g in $\mathcal{F}\{z\}$ of positive class and algebraically irreducible, there is only one essential prime divisor of $\{g\}$ which does not contain S_g ; the manifold of this prime differential ideal is called the *general solution of g* (see [23, Ch. II, §12-16]).

2.3 Hilbert-Kolchin function and differentiation index

Let \mathfrak{P} be a prime differential ideal of $\mathcal{F}\{z\}$. The *differential dimension* of \mathfrak{P} , denoted by $\text{diffdim}(\mathfrak{P})$, is the differential transcendence degree of the extension $\mathcal{F} \hookrightarrow \text{Frac}(\mathcal{F}\{z\}/\mathfrak{P})$ (where Frac denotes the fraction field). The *differential Hilbert-Kolchin function* of \mathfrak{P} with respect to \mathcal{F} is the function $H_{\mathfrak{P}, \mathcal{F}} : \mathbb{N}_0 \rightarrow \mathbb{N}_0$ defined as:

$$H_{\mathfrak{P}, \mathcal{F}}(i) := \text{the (algebraic) transcendence degree of } \text{Frac}(\mathcal{F}[z^{[i]})/(\mathfrak{P} \cap \mathcal{F}[z^{[i]}]) \text{ over } \mathcal{F}.$$

For $i \gg 0$, this function equals the linear function $\text{diffdim}(\mathfrak{P})(i + 1) + \text{ord}(\mathfrak{P})$, where $\text{ord}(\mathfrak{P}) \in \mathbb{N}_0$ is an invariant called the *order* of \mathfrak{P} ([14, Ch. II, Sec. 12, Theorem 6]). The minimum i from which this equality holds is the Hilbert-Kolchin *regularity* of \mathfrak{P} .

Let F be a finite set of differential polynomials contained in \mathfrak{P} of order bounded by a non-negative integer e . Throughout the paper we assume that $e \geq 1$, in other words, all the systems we consider are actually differential but no purely algebraic.

Definition 1 *The set F is quasi-regular at \mathfrak{P} if, for every $k \in \mathbb{N}_0$, the Jacobian matrix of the polynomials $F, \dot{F}, \dots, F^{(k)}$ with respect to the variables $z^{[e+k]}$ has full row rank over the fraction field of $\mathcal{F}\{z\}/\mathfrak{P}$.*

A fundamental invariant associated to ordinary differential algebraic equation systems is the *differentiation index*. There are several definitions of this notion (see [4] and the references given there), but in every case it represents a measure of the implicitness of the given system. Here we will use the following definition, introduced in [4, Section 3], in the context of quasi-regular systems (i.e. finite sets of differential polynomials) with respect to a fixed prime differential ideal \mathfrak{P} :

Definition 2 *The \mathfrak{P} -differentiation index σ of a quasi-regular system F of polynomials in $\mathcal{F}\{z\}$ of order at most e is*

$$\sigma := \min\{k \in \mathbb{N}_0 : (F, \dot{F}, \dots, F^{(k)})_{\mathfrak{P}_e} \cap \mathcal{F}[z^{[e]}]_{\mathfrak{P}_e} = [F]_{\mathfrak{P}} \cap \mathcal{F}[z^{[e]}]_{\mathfrak{P}_e}\},$$

where $\mathfrak{P}_e := \mathfrak{P} \cap \mathcal{F}[z^{[e]}]$ (i.e. the contraction of the prime ideal \mathfrak{P}) and $\mathcal{F}[z^{[e]}]_{\mathfrak{P}_e}$ denotes the localized ring at the prime ideal \mathfrak{P}_e .

3 Differential Lüroth's Theorem

In [22, Chapter VIII] (see also [14] and [23]), the classical Lüroth's Theorem for transcendental field extensions is generalized to the differential algebra framework:

Theorem 3 (Differential Lüroth's Theorem) *Let \mathcal{F} be a differential field of characteristic 0 and let u be differentially transcendental over \mathcal{F} . Let \mathcal{G} be a differential field such that $\mathcal{F} \subset \mathcal{G} \subset \mathcal{F}\langle u \rangle$. Then, there is an element $v \in \mathcal{G}$ such that $\mathcal{G} = \mathcal{F}\langle v \rangle$.*

Our goal is the following: for $n > 1$, let be given differential polynomials $P_1, \dots, P_n, Q_1, \dots, Q_n \in \mathcal{F}\{u\}$, with $P_j/Q_j \notin \mathcal{F}$ and P_j, Q_j relatively prime polynomials for every $1 \leq j \leq n$, and denote

$$\mathcal{G} := \mathcal{F}\langle P_1(u)/Q_1(u), \dots, P_n(u)/Q_n(u) \rangle,$$

which is a subfield of $\mathcal{F}\langle u \rangle$. We want to compute a Lüroth generator of \mathcal{G}/\mathcal{F} , that is, a pair of differential polynomials $P, Q \in \mathcal{F}\{u\}$ such that $Q \not\equiv 0$ and $\mathcal{G} = \mathcal{F}\langle P(u)/Q(u) \rangle$. We are also interested in the study of *a priori* upper bounds for the orders and degrees of both polynomials P and Q .

We start by discussing some ingredients which appear in the classical proofs of Theorem 3 (see [23, 15]) and that we also consider in our approach.

Following [23, II. §39], let y be a new differential indeterminate and consider the differential prime ideal of all differential polynomials in $\mathcal{G}\{y\}$ vanishing at u :

$$\Sigma = \{A \in \mathcal{G}\{y\} \text{ such that } A(u) = 0\}.$$

Lemma 4 *The manifold of Σ is the general solution of an irreducible differential polynomial $B \in \mathcal{G}\{y\}$. More precisely, B is a differential polynomial in Σ with the lowest rank in y .*

Proof. Let $B \in \Sigma$ be a differential polynomial with the lowest rank in y . Note that $B \in \mathcal{G}\{y\}$ is algebraically irreducible, since Σ is prime. We denote the order of B by k and the separant of B by $S_B = \partial B / \partial y^{(k)}$. Consider the differential ideal

$$\Sigma_1(B) := \{A \in \mathcal{G}\{y\} \mid S_B A \equiv 0 \pmod{\{B\}}\}.$$

As shown in [23, II. §12], the ideal $\Sigma_1(B)$ is prime; moreover, we have that $A \in \Sigma_1(B)$ if and only if $S_B^a A \equiv 0 \pmod{[B]}$ for some $a \in \mathbb{N}_0$ and, in particular, if $A \in \Sigma_1(B)$ is of order at most $k = \text{ord}(B)$, then A is a multiple of B (see [23, II. §13]). Furthermore, $\Sigma_1(B)$ is an essential prime divisor of $\{B\}$ and, in the representation of $\{B\}$ as an intersection of its essential prime divisors, it is the only prime which does not contain S_B ([23, II. §15]).

In order to prove the lemma, it suffices to show that $\Sigma = \Sigma_1(B)$.

Let $A \in \Sigma_1(B)$. Then, $S_B A \in \{B\}$. Taking into account that Σ is prime, $\{B\} \subset \Sigma$, and $S_B \notin \Sigma$, it follows that $A \in \Sigma$.

To see the other inclusion, consider a differential polynomial $A \in \Sigma$. By the minimality of B , we have that A is of rank at least the rank of B . Reducing A modulo B , we obtain a relation of the type

$$S_B^b I_B^c A \equiv R \pmod{[B]},$$

where $b, c \in \mathbb{N}_0$, I_B is the initial of B and R is a differential polynomial whose rank is lower than the rank of B . Since A and B lie in the differential ideal Σ , it follows that $R \in \Sigma$, and so, the minimality of B implies that $R = 0$. In particular, $S_B^b I_B^c A \in [B]$ and, therefore, $I_B^c A \in \Sigma_1(B)$. Now, $I_B \notin \Sigma_1(B)$ since, otherwise, it would be a differential polynomial in Σ with a rank lower than the rank of B (recall that $\Sigma_1(B) \subset \Sigma$); it follows that $A \in \Sigma_1(B)$. ■

Multiplying the polynomial $B \in \mathcal{G}\{y\}$ by a suitable denominator, we obtain a differential polynomial $C \in \mathcal{F}\{u, y\}$ with no factor in $\mathcal{F}\{u\}$. The following result is proved in [23, II. §42]:

Lemma 5 *If $P(u)$ and $Q(u) \neq 0$ are two coefficients of C (regarded as a polynomial in $\mathcal{F}\{u\}\{y\}$) such that $P(u)/Q(u) \notin \mathcal{F}$, the polynomial*

$$D(u, y) := Q(u)P(y) - P(u)Q(y)$$

is a multiple of C by a factor in \mathcal{F} , and $\mathcal{G} = \mathcal{F}\langle P(u)/Q(u) \rangle$. ■

Note that, by the definition of C , the ratio between two coefficients of C coincides with the ratio of the corresponding coefficients of B .

Under our assumptions, consider the map of differential algebras defined by

$$\begin{array}{ccc} \psi : \mathcal{F}\{x_1, \dots, x_n, u\} & \rightarrow & \mathcal{F}\{P_1(u)/Q_1(u), \dots, P_n(u)/Q_n(u), u\} \\ x_i & \mapsto & P_i(u)/Q_i(u) \\ u & \mapsto & u \end{array}$$

Let $\mathfrak{P} \subset \mathcal{F}\{x, u\}$ be the kernel of the morphism ψ ; then, we have an isomorphism

$$\mathcal{F}\{P_1(u)/Q_1(u), \dots, P_n(u)/Q_n(u), u\} \simeq \mathcal{F}\{x_1, \dots, x_n, u\}/\mathfrak{P}.$$

This implies that \mathfrak{P} is a *prime* differential ideal. In addition, this isomorphism gives an inclusion

$$\mathcal{F}\{P_1(u)/Q_1(u), \dots, P_n(u)/Q_n(u)\} \hookrightarrow \mathcal{F}\{x_1, \dots, x_n, u\}/\mathfrak{P},$$

and the inclusion induced from this map in the fraction fields leads to the original extension $\mathcal{G} = \mathcal{F}\langle P_1(u)/Q_1(u), \dots, P_n(u)/Q_n(u) \rangle \hookrightarrow \mathcal{F}\langle u \rangle$ since \mathfrak{P} does not contain non trivial polynomials in $\mathcal{F}\{u\}$.

Now, if $A \in \mathcal{G}\{y\}$ is a differential polynomial in Σ , multiplying it by an adequate element in $\mathcal{F}\{P_1(u)/Q_1(u), \dots, P_n(u)/Q_n(u)\}$, we obtain a differential polynomial in $\mathcal{F}\{P_1(u)/Q_1(u), \dots, P_n(u)/Q_n(u)\}\{y\}$, with the same rank in y as A . Taking a representative in $\mathcal{F}\{x_1, \dots, x_n\}$ for each of its coefficients, we get a differential polynomial $\tilde{A} \in \mathcal{F}\{x_1, \dots, x_n, u\}$, with the same rank in y as A , such that $\tilde{A} \in \mathfrak{P}$. Conversely, from a differential polynomial $M \in \mathcal{F}\{x_1, \dots, x_n, u\}$ such that $M \in \mathfrak{P}$, we may obtain a differential polynomial

$$\tilde{M}(y) := M(P_1(u)/Q_1(u), \dots, P_n(u)/Q_n(u), y) \in \mathcal{G}\{y\} \quad (1)$$

vanishing at u , with a rank in y no higher than that of M . Notice that $\tilde{M} \in \mathcal{F}(u^{[2e]})[y^{[2e]}]$, since $\text{ord}(M) \leq e$ and $\text{ord}(P_j/Q_j) \leq e$ for every $1 \leq j \leq n$.

We conclude that if $M \in \mathcal{F}\{x_1, \dots, x_n, u\}$ is a differential polynomial in \mathfrak{P} with the lowest rank in u , the associated differential polynomial $\tilde{M}(y)$ is a multiple by a factor in \mathcal{G} of the minimal polynomial B of u over \mathcal{G} . Therefore, a Lüroth generator of \mathcal{G}/\mathcal{F} can be obtained as the ratio of any pair of coefficients of $\tilde{M} \in \mathcal{G}\{y\}$ provided this ratio does not lie in \mathcal{F} . Moreover:

Proposition 6 *Let $M \in \mathcal{F}\{x_1, \dots, x_n, u\}$ be a differential polynomial in \mathfrak{P} with the lowest rank in u . Consider two generic points $u_1, u_2 \in \mathbb{Q}^{2e+1}$. Let M_1 and M_2 be the polynomials obtained by specializing M as in (1) and substituting $u^{[2e]}$ for u_1 and u_2 respectively in the polynomial obtained. Then $M_1(u)/M_2(u)$ is a Lüroth generator of \mathcal{G}/\mathcal{F} .*

Proof. By Lemma 5, we have that

$$\tilde{M}(y) = M(P_1(u)/Q_1(u), \dots, P_n(u)/Q_n(u), y) = \gamma(Q(u)P(y) - P(u)Q(y))$$

for some $\gamma \in \mathcal{G}$, and P, Q are such that $\mathcal{G} = \mathcal{F}\langle P(u)/Q(u) \rangle$. Then, by means of two suitable specializations u_1, u_2 of the variables $u^{[2e]}$ (so that Q_1, \dots, Q_n, Q and γ do not vanish and $P(u_1)/Q(u_1) \neq P(u_2)/Q(u_2)$), we obtain polynomials of the form

$$M_1(y) = \alpha_1 P(y) - \beta_1 Q(y) \quad \text{and} \quad M_2(y) = \alpha_2 P(y) - \beta_2 Q(y),$$

where $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathcal{F}$ and $\alpha_1\beta_2 - \alpha_2\beta_1 \neq 0$. The proposition follows since $\mathcal{F}\langle M_1(u)/M_2(u) \rangle = \mathcal{F}\langle P(u)/Q(u) \rangle = \mathcal{G}$. ■

For every j , $1 \leq j \leq n$, denote $F_j := Q_j(u)x_j - P_j(u) \in \mathcal{F}\{x, u\}$, and let $F := F_1, \dots, F_n$. Then we have:

Lemma 7 *The ideal \mathfrak{P} is the (unique) minimal differential prime ideal of $[F]$ which does not contain the product $Q_1 \dots Q_n$. Moreover, $\mathfrak{P} = [F] : (Q_1 \dots Q_n)^\infty$.*

Proof. From the definitions of \mathfrak{P} and F it is clear that $[F] \subset \mathfrak{P}$ and $Q_1(u) \dots Q_n(u) \notin \mathfrak{P}$. Moreover, since F is a characteristic set for the order in $\mathcal{F}\{x, u\}$ given by $u < x_1 < \dots < x_n$ and $\mathfrak{P} \cap \mathcal{F}\{u\} = (0)$, we conclude that for any polynomial $H \in \mathfrak{P}$ there exists $N \in \mathbb{N}_0$ such that $(Q_1(u) \dots Q_n(u))^N H \in [F]$ (observe that Q_j is the initial and the separant of the polynomial F_j for every j). The proposition follows. ■

Moreover, we have the following property that we will use in the sequel (recall Definition 1):

Lemma 8 *The system F is quasi-regular at \mathfrak{P} .*

Proof. Let e be the maximum of the orders of the differential polynomials F_j , $1 \leq j \leq n$. For every $i \in \mathbb{N}$, let J_i be the Jacobian matrix of the polynomials $F^{[i-1]}$ with respect to the variables $(x, u)^{[i-1+e]}$. We have that

$$\frac{\partial F_j^{(k)}}{\partial x_h^{(l)}} = \begin{cases} 0 & \text{if } h \neq j \text{ or } h = j, k < l \\ \binom{k}{l} Q_j^{(k-l)} & \text{if } h = j, k \geq l \end{cases}$$

and so, for every $i \in \mathbb{N}$, the minor of J_i corresponding to partial derivatives with respect to the variables $x^{[i-1]}$ is a scalar multiple of $(Q_1(u) \dots Q_n(u))^i$, which is not zero modulo \mathfrak{P} . ■

4 Bounding the orders

Here we estimate the order in the variables $x = x_1, \dots, x_n$ and u of a differential polynomial $M(x, u) \in \mathfrak{P}$ of minimal rank in u and the order of a Lüroth generator of the differential extension \mathcal{G}/\mathcal{F} .

Let $e := \max\{\text{ord}(P_j/Q_j) : 1 \leq j \leq n\}$. Without loss of generality, we may assume that $\text{ord}(P_1(u)/Q_1(u)) \geq \dots \geq \text{ord}(P_n(u)/Q_n(u))$. Consider the elimination order in $\mathcal{F}\{x_1, \dots, x_n, u\}$ with $x_1 < \dots < x_n < u$.

Taking into account that the fraction field of $\mathcal{F}\{x_1, \dots, x_n, u\}/\mathfrak{P}$ is isomorphic to $\mathcal{F}\langle u \rangle$, we deduce that the differential dimension of \mathfrak{P} equals 1. Since $P_1(u)/Q_1(u) \notin \mathcal{F}$, it is transcendental over \mathcal{F} . Now, as the variable $u^{(e+1)}$ appears in the derivative $(P_1(u)/Q_1(u))'$ but it does not appear in $P_1(u)/Q_1(u)$, it follows that $(P_1(u)/Q_1(u))'$ is (algebraically) transcendental over $\mathcal{F}(P_1(u)/Q_1(u))$. Continuing in the same way with the successive derivatives, we conclude that $P_1(u)/Q_1(u)$ is differentially transcendental over \mathcal{F} . This implies that the differential ideal \mathfrak{P} contains no differential polynomial involving only the variable x_1 .

Thus, a characteristic set of \mathfrak{P} for the considered elimination order is of the form

$$R_1(x_1, x_2), R_2(x_1, x_2, x_3), \dots, R_{n-1}(x_1, \dots, x_n), R_n(x_1, \dots, x_n, u).$$

Furthermore, $R_n(x_1, \dots, x_n, u)$ is a differential polynomial in \mathfrak{P} with a minimal rank in u , that is, we can take $M(x, u) = R_n(x, u)$. Following [24, Lemma 19], we may assume this

characteristic set to be irreducible. Then, by [24, Theorem 24], we have that $\text{ord}(R_i) \leq \text{ord}(\mathfrak{P})$ for every $1 \leq i \leq n$; in particular,

$$\text{ord}(M) \leq \text{ord}(\mathfrak{P}). \quad (2)$$

The order of the differential prime ideal \mathfrak{P} can be computed exactly:

Proposition 9 *The order of the differential ideal \mathfrak{P} equals $e = \max\{\text{ord}(P_j(u)/Q_j(u)) : 1 \leq j \leq n\}$.*

Proof. Lemma 7 states that the ideal \mathfrak{P} is an essential prime divisor of $[F]$, where $F = F_1, \dots, F_n$ with $F_j(x, u) := Q_j(u)x_j - P_j(u)$, $1 \leq j \leq n$, and, as shown in Lemma 8, the system F is quasi-regular at \mathfrak{P} . Therefore, taking into account that e is the maximum of the orders of the polynomials in F , by [4, Theorem 12], the regularity of the Hilbert-Kolchin function of \mathfrak{P} is at most $e - 1$. This implies that the order of \mathfrak{P} can be obtained from the value of this function at $e - 1$; more precisely, since the differential dimension of \mathfrak{P} equals 1, we have that

$$\text{ord}(\mathfrak{P}) = \text{trdeg}_{\mathcal{F}} \left(\mathcal{F}[x^{[e-1]}, u^{[e-1]}] / (\mathfrak{P} \cap \mathcal{F}[x^{[e-1]}, u^{[e-1]}]) \right) - e.$$

In order to compute the transcendence degree involved in the above formula, we observe first that $\mathcal{F}[x^{[e-1]}, u^{[e-1]}] / (\mathfrak{P} \cap \mathcal{F}[x^{[e-1]}, u^{[e-1]}]) \simeq \mathcal{F}[(P_j/Q_j)^{[e-1]}, u^{[e-1]}]$.

It is clear that the variables $u^{[e-1]}$ are algebraically independent in this ring. Then, if $L = \mathcal{F}(u^{[e-1]})$, the order of the ideal \mathfrak{P} coincides with the transcendence degree of $L((P_j/Q_j)^{[e-1]}, j = 1, \dots, n)$ over L . Without loss of generality, we may assume that $\text{ord}(P_1/Q_1) = e$. Since the variable $u^{(e)}$ appears in P_1/Q_1 , we have that $L(u^{(e)})/L(P_1/Q_1)$ is algebraic. Similarly, since $u^{(e+1)}$ appears in $(P_1/Q_1)'$, it follows that the extension $L(u^{(e)}, u^{(e+1)})/L((P_1/Q_1), (P_1/Q_1)')$ is algebraic. Proceeding in the same way with the successive derivatives of P_1/Q_1 , we conclude that $L(u^{(e)}, u^{(e+1)}, \dots, u^{(2e-1)})$ is algebraic over $L((P_1/Q_1)^{[e-1]})$.

Since $\text{ord}(P_j/Q_j) \leq e$ for $j = 1, \dots, n$, we have that $L((P_j/Q_j)^{[e-1]}, j = 1, \dots, n) \subset L(u^{(e)}, u^{(e+1)}, \dots, u^{(2e-1)})$ and, by the arguments in the previous paragraph, this extension is algebraic. Therefore,

$$\text{trdeg}_L L((P_j/Q_j)^{[e-1]}, j = 1, \dots, n) = \text{trdeg}_L L(u^{(e)}, u^{(e+1)}, \dots, u^{(2e-1)}) = e.$$

■

Then, by inequality (2) we conclude:

Corollary 10 *There is a differential polynomial $M \in \mathfrak{P} \subset \mathcal{F}\{x_1, \dots, x_n, u\}$ with the lowest rank in u such that $\text{ord}(M) \leq e$.*

Combining this corollary with the construction in Proposition 6, it is not too difficult to obtain the upper bound e for the order of the Lüroth generator $M_1(u)/M_2(u)$ of \mathcal{G}/\mathcal{F} . However, the following stronger result holds:

Proposition 11 *Under the previous assumptions and notation, any element $v \in \mathcal{G}$ such that $\mathcal{G} = \mathcal{F}\langle v \rangle$ satisfies $\text{ord}(v) \leq \min\{\text{ord}(P_j/Q_j) : 1 \leq j \leq n\}$.*

Proof. Let $v \in \mathcal{G}$ be such that $\mathcal{G} = \mathcal{F}\langle v \rangle$ and $\varepsilon := \text{ord}(v)$.

For $j = 1, \dots, n$, let $v_j = P_j(u)/Q_j(u)$. By assumption, $v_j \notin \mathcal{F}$; let $e_j := \text{ord}(v_j)$. Let T be a new differential indeterminate over \mathcal{F} . Since $v_j \in \mathcal{G} = \mathcal{F}\langle v \rangle$, there exists $\Theta_j \in \mathcal{F}\langle T \rangle$ such that $v_j = \Theta_j(v)$. Let $N_j = \text{ord}(\Theta_j)$.

Assuming $\varepsilon > e_j$, we have that $N_j + \varepsilon > e_j$ and, therefore,

$$0 = \frac{\partial v_j}{\partial u^{(N_j+\varepsilon)}} = \frac{\partial(\Theta_j(v))}{\partial u^{(N_j+\varepsilon)}} = \sum_{i \geq 0} \frac{\partial \Theta_j}{\partial T^{(i)}}(v) \frac{\partial v^{(i)}}{\partial u^{(N_j+\varepsilon)}} = \frac{\partial \Theta_j}{\partial T^{(N_j)}}(v) \frac{\partial v^{(N_j)}}{\partial u^{(N_j+\varepsilon)}}.$$

Since N_j is the order of Θ_j , it follows that $\frac{\partial \Theta_j}{\partial T^{(N_j)}} \neq 0$, and as v is differentially transcendental over \mathcal{F} , we have that $\frac{\partial \Theta_j}{\partial T^{(N_j)}}(v) \neq 0$. We conclude that $\frac{\partial v^{(N_j)}}{\partial u^{(N_j+\varepsilon)}} = 0$, which leads to a contradiction. ■

Note that the proof of the above proposition shows that all possible Lüroth generators v have the same order. In fact, two arbitrary generators are related by an homographic map with coefficients in \mathcal{F} (see for instance [15, §1], [23, Ch. II, §44]).

5 Bounding the total degree

5.1 Reduction to algebraic polynomial ideals

As stated in Proposition 6, the Lüroth generator of \mathcal{G}/\mathcal{F} is closely related with a polynomial $M(x_1, \dots, x_n, u) \in \mathfrak{P}$ with the lowest rank in u .

By Corollary 10, such a polynomial M can be found in the algebraic ideal $\mathfrak{P} \cap \mathcal{F}[x^{[e]}, u^{[e]}]$ of the polynomial ring $\mathcal{F}[x^{[e]}, u^{[e]}]$. The following result will enable us to work with a finitely generated ideal given by known generators; the key point is the estimation of the \mathfrak{P} -differentiation index of the system $F := F_1, \dots, F_n$ (see Definition 2):

Lemma 12 *The \mathfrak{P} -differentiation index of F equals e . In particular, if $\mathfrak{P}_e := \mathfrak{P} \cap \mathcal{F}[x^{[e]}, u^{[e]}]$, we have that $[F]_{\mathfrak{P}} \cap \mathcal{F}[x^{[e]}, u^{[e]}]_{\mathfrak{P}_e} = (F, \dot{F}, \dots, F^{(e)})_{\mathfrak{P}_e} \cap \mathcal{F}[x^{[e]}, u^{[e]}]_{\mathfrak{P}_e}$.*

Proof. For every $k \in \mathbb{N}$, let \mathfrak{J}_k be the Jacobian submatrix of the polynomials $F, \dots, F^{(k-1)}$ with respect to the variables $(x, u)^{(e)}, \dots, (x, u)^{(e+k-1)}$. The \mathfrak{P} -differentiation index of F can be obtained as the minimum k such that $\text{rank}(\mathfrak{J}_{k+1}) - \text{rank}(\mathfrak{J}_k) = n$, where the ranks are computed over the fraction field of $\mathcal{F}\{x, u\}/\mathfrak{P}$ (see [4, Section 3.1]).

Now, since the order of the polynomials F in the variables x is zero, no derivative $x^{(l)}$ with $l \geq e$ appears in $F, \dot{F}, \dots, F^{(e-1)}$. This implies that the columns of the Jacobian submatrices \mathfrak{J}_k of these systems corresponding to partial derivatives with respect to $x^{(l)}$, $l = e, \dots, e+k-1$, are null. On the other hand, as e is the order of the system F , we may suppose that the variable $u^{(e)}$ appears in the polynomial F_1 and so, $\partial F_1 / \partial u^{(e)} \neq 0$. Thus,

$\partial F_1^{(i)}/\partial u^{(h)} \neq 0$ for $h - i = e$ and $\partial F_j^{(i)}/\partial u^{(h)} = 0$ for $h - i > e$; that is, the matrices \mathfrak{J}_k , $k = 1, \dots, e$, are block, lower triangular matrices of the form

$$\mathfrak{J}_k = \begin{pmatrix} 0 & \cdots & 0 & * \\ 0 & \cdots & 0 & \star & 0 & \cdots & 0 & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots \\ 0 & \cdots & 0 & \star & 0 & \cdots & 0 & \star & \cdots & 0 & \cdots & 0 & * \end{pmatrix}$$

where 0 denotes a zero column vector and $*$ a non-zero column vector. Then, $\text{rank}(\mathfrak{J}_k) = k$ for $k = 1, \dots, e$. Moreover,

$$\mathfrak{J}_{e+1} = \begin{pmatrix} \mathfrak{J}_e \\ \frac{\partial F^{(e)}}{\partial x^{(e)}} & \cdots & \cdots & 0 & \cdots & 0 & * \end{pmatrix}$$

and, by the diagonal structure of

$$\frac{\partial F^{(e)}}{\partial x^{(e)}} = \begin{pmatrix} Q_1(u) & 0 & \cdots & 0 \\ 0 & Q_2(u) & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & Q_n(u) \end{pmatrix},$$

we see that $\text{rank}(\mathfrak{J}_{e+1}) = \text{rank}(\mathfrak{J}_e) + n$.

It follows that the \mathfrak{P} -differentiation index of the system equals e . ■

Notation 13 We denote by $\mathbb{V} \subset \mathbb{A}^{(e+1)n} \times \mathbb{A}^{2e+1}$ the affine variety defined as the Zariski closure of the solution set of the polynomial system $F = 0, \dot{F} = 0, \dots, F^{(e)} = 0, \prod_{1 \leq j \leq n} Q_j \neq 0$, where $F = F_1, \dots, F_n$ and $F_j(x, u^{[e]}) = Q_j(u^{[e]})x_j - P_j(u^{[e]})$ for every $1 \leq j \leq n$.

The algebraic ideal corresponding to the variety \mathbb{V} is $(F, \dot{F}, \dots, F^{(e)}) : q^\infty$, where $q := \prod_{1 \leq j \leq n} Q_j$. This ideal is prime, since it is the kernel of the map

$$\begin{aligned} \mathcal{F}[x^{[e]}, u^{[2e]}] &\rightarrow \mathcal{F}[(P_j/Q_j)_{1 \leq j \leq n}^{[e]}, u^{[2e]}] \\ x_j^{(k)} &\mapsto (P_j/Q_j)^{(k)} \\ u^{(i)} &\mapsto u^{(i)} \end{aligned}$$

Then, \mathbb{V} is an irreducible variety. Moreover, $F, \dot{F}, \dots, F^{(e)}$ is a reduced complete intersection in $\{q \neq 0\}$ and so, the dimension of \mathbb{V} is $2e + 1$. With the notations of Lemma 12 we have:

Lemma 14 The following equality of ideals holds: $(F, \dot{F}, \dots, F^{(e)}) : q^\infty \cap \mathcal{F}[x^{[e]}, u^{[e]}] = (F, \dot{F}, \dots, F^{(e)})_{\mathfrak{P}_e} \cap \mathcal{F}[x^{[e]}, u^{[e]}]$.

Proof. First note that $(F, \dot{F}, \dots, F^{(e)}) : q^\infty \subset (F, \dot{F}, \dots, F^{(e)})_{\mathfrak{P}_e}$ since $q \notin \mathfrak{P}$. Conversely, if $h \in (F, \dot{F}, \dots, F^{(e)})_{\mathfrak{P}_e} \cap \mathcal{F}[x^{[e]}, u^{[e]}]$, which is a prime ideal (see [4, Proposition 3]), there is a polynomial $g \in \mathcal{F}[x^{[e]}, u^{[e]}]$ such that $g \notin \mathfrak{P}_e$ and $gh \in (F, \dot{F}, \dots, F^{(e)})$; but $g \notin (F, \dot{F}, \dots, F^{(e)}) : q^\infty$, since otherwise, $q^N g \in (F, \dot{F}, \dots, F^{(e)}) \subset \mathfrak{P}$ for some $N \in \mathbb{N}$ contradicting the fact that $q \notin \mathfrak{P}$ and $g \notin \mathfrak{P}$. Now, Lemma 12 implies that

$$(F, \dot{F}, \dots, F^{(e)})_{\mathfrak{P}_e} \cap \mathcal{F}[x^{[e]}, u^{[e]}] = [F]_{\mathfrak{P}} \cap \mathcal{F}[x^{[e]}, u^{[e]}].$$

Finally, since $[F]_{\mathfrak{P}} \mathcal{F}\{x, u\}_{\mathfrak{P}} = \mathfrak{P}_{\mathfrak{P}} \mathcal{F}\{x, u\}_{\mathfrak{P}}$ (see [4, Proposition 3]), we conclude that

$$[F]_{\mathfrak{P}} \cap \mathcal{F}[x^{[e]}, u^{[e]}] = \mathfrak{P}_{\mathfrak{P}} \cap \mathcal{F}[x^{[e]}, u^{[e]}] = \mathfrak{P} \cap \mathcal{F}[x^{[e]}, u^{[e]}] = \mathfrak{P}_e.$$

Therefore,

$$(F, \dot{F}, \dots, F^{(e)}) : q^\infty \cap \mathcal{F}[x^{[e]}, u^{[e]}] = \mathfrak{P}_e.$$

■

5.2 Degree bounds

From Proposition 6, in order to estimate the degree of a Lüroth generator it suffices to know the degree of the minimal polynomial M . For this, we will interpret M as an eliminating polynomial for the algebraic variety \mathbb{V} under a suitable linear projection.

Consider a finite set of variables $\mathcal{B}_0 \subseteq \{x^{[e]}, u^{[e]}\}$ constructed in the following way. Let Z be a maximal subset of $\{x^{[e]}\}$ which is algebraically independent over \mathcal{F} as elements of the field $\mathcal{F}(\mathbb{V})$ of rational functions over \mathbb{V} , and U a maximal subset of $\{u^{[e]}\}$ such that $\{Z, U\}$ is algebraically independent over \mathcal{F} . Take $\mathcal{B}_0 := \{Z, U\}$.

Proposition 15 *The set $\mathcal{B}_0 \subseteq \{x^{[e]}, u^{[e]}\}$ induces a transcendence basis of $\mathcal{F}(\mathbb{V})$ over \mathcal{F} .*

Proof. First, note that the canonical morphism

$$\mathcal{F}[x^{[e]}, u^{[e]}] / (\mathfrak{P} \cap \mathcal{F}[x^{[e]}, u^{[e]}]) \rightarrow \mathcal{F}[x^{[e]}, u^{[2e]}] / (F, \dots, F^{(e)}) : q^\infty = \mathcal{F}[\mathbb{V}]$$

is injective (Lemmata 12 and 14). In particular \mathcal{B}_0 is a transcendence basis of the fraction field of $\mathcal{F}[x^{[e]}, u^{[e]}] / (\mathfrak{P} \cap \mathcal{F}[x^{[e]}, u^{[e]}])$.

On the other hand, from [4, Theorem 12], the order upper bound e is also an upper bound for the Hilbert regularity of \mathfrak{P} . Hence

$$\text{trdeg}_{\mathcal{F}} \mathcal{F}[x^{[e]}, u^{[e]}] / (\mathfrak{P} \cap \mathcal{F}[x^{[e]}, u^{[e]}]) = (e + 1) + \text{ord}(\mathfrak{P}) = 2e + 1,$$

as $\text{ord}(\mathfrak{P}) = e$ (see Proposition 9), and therefore the cardinality of \mathcal{B}_0 is $2e + 1$.

Since $2e + 1 = \dim(\mathbb{V}) = \text{trdeg}_{\mathcal{F}} \mathcal{F}(\mathbb{V})$ the proposition follows. ■

Let $k_0 := \min\{k : u^{(k)} \notin \mathcal{B}_0\}$. By Corollary 10, we have that $k_0 \leq e$. Consider the projection

$$\pi : \mathbb{V} \rightarrow \mathbb{A}^{2e+2}, \quad \pi(x^{[e]}, u^{[2e]}) = (Z, U, u^{(k_0)}). \quad (3)$$

Then, from Proposition 15, the Zariski closure of $\pi(\mathbb{V})$ is a hypersurface in \mathbb{A}^{2e+2} and a square-free polynomial defining this hypersurface is the minimal polynomial $M(x, u)$ we are looking for. In particular we have the inequality

$$\deg M \leq \deg \mathbb{V}$$

(see [11, Lemma 2]) and we can exhibit purely syntactic degree bounds of \mathbb{V} in terms of the number n of given generators for \mathcal{G}/\mathcal{F} , their maximum order e , and an upper bound d for the degrees of their numerators and denominators.

First, since the variety \mathbb{V} is an irreducible component of the algebraic set defined by the $(e+1)n$ polynomials $F, \bar{F}, \dots, F^{(e)}$ of total degrees bounded by $d+1$ (here $F = F_1, \dots, F_n$ and $F_j(x, u) = Q_j(u)x_j - P_j(u)$), Bézout's theorem (see for instance [11, Theorem 1]) implies that

$$\deg \mathbb{V} \leq (d+1)^{(e+1)n}.$$

An analysis of the particular structure of the system leads to a different upper bound for $\deg(\mathbb{V})$, which is not exponential in n : taking into account that \mathbb{V} is an irreducible variety of dimension $2e+1$, its degree is the number of points in its intersection with a generic linear variety of codimension $2e+1$, that is,

$$\deg \mathbb{V} = \#(\mathbb{V} \cap V(L_1, \dots, L_{2e+1})),$$

where, for every $1 \leq i \leq 2e+1$, L_i is a generic affine linear form in the variables $x^{[e]}, u^{[2e]}$,

$$L_i(x^{[e]}, u^{[2e]}) = \sum_{\substack{1 \leq j \leq n \\ 0 \leq k \leq e}} a_{ijk} x_j^{(k)} + \sum_{0 \leq k \leq 2e} b_{ik} u^{(k)} + c_i. \quad (4)$$

For every $1 \leq j \leq n$, the equation $F_j(x_j, u) = 0$ implies that, generic points of \mathbb{V} satisfy $x_j = P_j(u)/Q_j(u)$. Proceeding inductively, it follows easily that, generically

$$x_j^{(k)} = \left(\frac{P_j(u)}{Q_j(u)} \right)^{(k)} = \frac{R_{jk}(u^{[e+j]})}{Q_j(u^{[e]})^{k+1}} \quad \text{with } \deg(R_{jk}) \leq d(k+1)$$

for every $1 \leq j \leq n$, $0 \leq k \leq e$. Substituting these formulae into (4) and clearing denominators, we deduce that the degree of \mathbb{V} equals the number of common solutions of the system defined by the $2e+1$ polynomials

$$\begin{aligned} \mathbb{L}_i(u^{[2e]}) &:= \left(\prod_{1 \leq j \leq n} Q_j^{e+1} \right) L_i \left(\left(\frac{P_1}{Q_1}, \dots, \frac{P_n}{Q_n} \right)^{[e]}, u^{[2e]} \right) \\ &= \sum_{\substack{1 \leq j \leq n \\ 0 \leq k \leq e}} a_{ijk} R_{jk} Q_j^{e-k} \prod_{h \neq j} Q_h^{e+1} + \sum_{0 \leq k \leq 2e} b_{ik} u^{(k)} \prod_{1 \leq j \leq n} Q_j^{e+1} + c_i \prod_{1 \leq j \leq n} Q_j^{e+1} \end{aligned}$$

for generic coefficients a_{ijk}, b_{ik}, c_i and the inequality $q \neq 0$. From the upper bounds for the degrees of the polynomials Q_j, R_{jk} , it follows that \mathbb{L}_i is a polynomial of total degree bounded by $nd(e+1)+1$ for every $1 \leq i \leq 2e+1$. Therefore, Bézout's bound implies that

$$\deg \mathbb{V} \leq (nd(e+1)+1)^{2e+1}.$$

Recalling that a Lüroth generator v of \mathcal{G}/\mathcal{F} can be obtained as the quotient of two specializations of the polynomial M (see Proposition 6) and that two arbitrary generators are related by an homographic map with coefficients in \mathcal{F} (see [15, §1], [23, Ch. II, §44]), we conclude that the previous upper bounds for $\deg \mathbb{V}$ are also upper bounds for the degrees of the numerator and the denominator of any Lüroth generator of \mathcal{G}/\mathcal{F} .

6 The algorithm

This section is devoted to presenting an algorithm for the computation of a Lüroth generator. The algorithm is based on the computation of the eliminating polynomial M associated to the projection π defined in (3) over the positive-dimensional irreducible variety \mathbb{V} .

Our algorithm relies on the computation of a *parametric geometric resolution* of the system defining \mathbb{V} as its main elimination step. Before proceeding, we briefly introduce this notion in our setting (for the general definition see [26, Section 2.1]).

Let $\mathcal{B} \subset \{x^{[e]}, u^{[2e]}\}$ be a transcendence basis of $\mathcal{F}(\mathbb{V})$ over \mathcal{F} ; then, $\mathcal{F}(\mathcal{B}) \hookrightarrow \mathcal{F}(\mathbb{V})$ is a finite algebraic extension. A parametric geometric resolution of \mathbb{V} with respect to \mathcal{B} consists in:

- a linear form ℓ in $\{x^{[e]}, u^{[2e]}\} \setminus \mathcal{B}$ which is a primitive element of $\mathcal{F}(\mathcal{B}) \hookrightarrow \mathcal{F}(\mathbb{V})$,
- the monic minimal polynomial $m_\ell \in \mathcal{F}(\mathcal{B})[T]$ of ℓ ,
- parametrizations of the algebraic variables in terms of ℓ , namely, for every variable $w \in \{x^{[e]}, u^{[2e]}\} \setminus \mathcal{B}$, a polynomial $V_w \in \mathcal{F}(\mathcal{B})[T]$ with $\deg V_w < \deg m_\ell$ such that $\frac{\partial m_\ell}{\partial T}(\ell)w = V_w(\ell)$ in $\mathcal{F}(\mathbb{V})$.

The data structure we use to represent multivariate polynomials is the *straight-line program* encoding. Roughly speaking, a straight-line program encoding a polynomial is a program which enables one to evaluate it at any given point. Each of the instructions in this program is an addition, subtraction or multiplication between two pre-calculated polynomials, or an addition or multiplication by a scalar. The number of instructions in the program is called the *length* of the straight-line program. For the precise definitions and basic properties we refer the reader to [2] (see also [13]).

Algorithm LurothGenerator

INPUT: A positive integer e , a straight-line program of length L encoding polynomials $P_1, Q_1, \dots, P_n, Q_n \in \mathcal{F}[u^{[e]}]$ such that $\mathcal{G} = \mathcal{F}\langle P_1(u)/Q_1(u), \dots, P_n(u)/Q_n(u) \rangle$, and an upper bound d for the total degrees of the polynomials P_j, Q_j .

OUTPUT: An element $v = M_1(u)/M_2(u) \in \mathcal{G}$ such that $\mathcal{G} = \mathcal{F}\langle v \rangle$.

PROCEDURE:

1. For $j = 1, \dots, n$, set $F_j(x, u) := Q_j(u)x_j - P_j(u)$.

2. Compute an slp encoding $F, \dot{F}, \dots, F^{(e)}$ and $q := \prod_{1 \leq j \leq n} Q_j$, where $F := F_1, \dots, F_n$.
3. Compute a transcendence basis $\mathcal{B}_0 = \{Z, U\}$ of $\mathcal{F}[x^{[e]}, u^{[2e]}]/(F, \dot{F}, \dots, F^{(e)}) : q^\infty$ over \mathcal{F} with $Z \subset x^{[e]}$ maximal and $U \subset u^{[e]}$.
4. Compute a parametric geometric resolution $m, (V_w)_{w \in \{x^{[e]}, u^{[2e]}\} \setminus \{Z, U\}} \in \mathcal{F}(\mathcal{B}_0)[T]$ of \mathbb{V} with respect to the parameters Z, U .
5. Set $k_0 := \min\{k : u^{(k)} \notin U\}$ and compute the minimal polynomial $M(Z, U, u^{(k_0)})$ of $u^{(k_0)}$ modulo $(F, \dot{F}, \dots, F^{(e)}) : q^\infty$.
6. From two random specializations of M , obtain polynomials $M_1(u), M_2(u) \in \mathcal{F}[u^{[e]}]$ such that $\mathcal{G} = \mathcal{F}\langle M_1(u)/M_2(u) \rangle$.

We now explain how the computations in the different steps of the algorithm are performed.

In Step 1, we use the input straight-line program in order to obtain a straight-line program of length $L+3n$ encoding F_1, \dots, F_n, q by simply computing, for each $j = 1, \dots, n$, a multiplication and a subtraction using the new variables x_1, \dots, x_n and previous results, and the product of the n polynomials Q_1, \dots, Q_n .

From this straight-line program, in Step 2, we can obtain a straight-line program of length $O(e^4n + e^2L)$ encoding all the successive derivatives $F, \dot{F}, \dots, F^{(e)}$ proceeding as in [5, Lemma 21] (see also [19, Section 5.2]).

The computation of the transcendence basis $\mathcal{B}_0 = \{Z, U\}$ involved in Step 3 relies on the well-known Jacobian criterion from commutative algebra [17, Chapter VI, Section 1, Theorem 1.15]; more precisely, we apply [5, Lemma 19]. Since $\mathcal{F}[x^{[e]}, u^{[2e]}]/(F, \dot{F}, \dots, F^{(e)}) : q^\infty \simeq \mathcal{F}[(P_1(u)/Q_1(u))^{[e]}, \dots, (P_n(u)/Q_n(u))^{[e]}, u^{[2e]}]$, it follows that all rank computations can be done in $\mathcal{F}(u^{[2e]})$. Therefore, we may proceed as in the proof of [5, Theorem 27]. The resulting subroutine is polynomial in e, n , and linear in L .

Step 4 is achieved by means of a slightly modified version of the algorithm in [26, Section 4] within a complexity polynomial in $n, e, d, \deg \mathbb{V}$ and linear in L . The algorithm proceeds in three main steps:

- (a) *Initial estimation:* Given a point $(\zeta, \nu) \in \mathbb{Q}^{2e+1}$, compute a geometric resolution of the simple roots of the system $F|_{(\zeta, \nu)} = 0, \dot{F}|_{(\zeta, \nu)} = 0, \dots, F^{(e)}|_{(\zeta, \nu)} = 0, q|_{(\zeta, \nu)} \neq 0$ obtained by specializing $(Z, U) = (\zeta, \nu)$.
- (b) *Approximation:* Starting from the solution of the specialized system, by means of a Newton-Hensel type procedure approximate the coefficients of the corresponding parametric resolution in a ring of formal power series.
- (c) *Reconstruction:* Recover the coefficients of the parametric geometric resolution from their power series expansion at (ζ, ν) .

In fact, our modification of the procedure in [26, Section 4] consists in the way we manipulate the objects in intermediate computations: we use straight-line programs to deal

with truncated power series. In particular, we modify step (c) of the algorithm, which is achieved by a multivariate Padé approximation procedure ([26, Section 4.3.1]), in order to work with the straight-line program encoding of polynomials, by replacing the Euclidean extended algorithm with subresultant computations (see [7, Section 5.9, Corollary 6.49]) as explained in the proof of [5, Proposition 46].

Once the parametric geometric resolution of \mathbb{V} is obtained, the computation of the minimal polynomial in Step 5 is straightforward (see, for instance, [12]) and can be done within the same complexity bounds.

We point out that the computation of the polynomial M could be performed, alternatively, from the polynomials $F, \dot{F}, \dots, F^{(e)}, q$ by a procedure based on an extension of the method presented in [12] (which assumes the projection to be a finite morphism) to the case of a dominant map by means of the techniques described in [26] (this approach can be found, for instance, in [5, Proposition 46]).

Finally, in Step 6 we specialize the variables x and its derivatives in $M(x, u)$ into the values obtained by choosing at random two sets u_1, u_2 of values for $u^{[2e]}$ and solving the linear system $F(x, u_i) = 0, \dot{F}(x, \dot{x}, u_i) = 0, \dots, F^{(e)}(x, \dot{x}, \dots, x^{(e)}, u_i) = 0$ in the unknowns $x^{[e]}$. In this way, we obtain polynomials $M_1(y), M_2(y)$ providing a Lüroth generator $v := M_1(u)/M_2(u)$ of \mathcal{G}/\mathcal{F} . Note that the matrices of the linear systems to be solved are the specializations at u_1, u_2 of the Jacobian matrices of $F, \dot{F}, \dots, F^{(e)}$ with respect to the variables $x^{[e]}$ with an additional column containing $F(0, u_i), \dots, F^{(e)}(0, u_i)$ and so, they can be computed from a straight-line program encoding the polynomials in polynomial time.

Therefore, we have the following complexity result:

Theorem 16 *Let \mathcal{F} be a differential field of characteristic 0 and u differentially transcendental over \mathcal{F} . Let $\mathcal{G} = \mathcal{F}\langle P_1(u)/Q_1(u), \dots, P_n(u)/Q_n(u) \rangle$, where $P_j, Q_j \in \mathcal{F}\{u\}$ are relatively prime differential polynomials of order at most e and total degree bounded by d such that $P_j/Q_j \notin \mathcal{F}$ for every $1 \leq j \leq n$. Algorithm **LurothGenerator** computes differential polynomials $M_1(u), M_2(u)$ of order and total degree bounded by $\min\{\text{ord}(P_j/Q_j); 1 \leq j \leq n\}$ and $\deg \mathbb{V}$ respectively, such that $\mathcal{G} = \mathcal{F}\langle M_1(u)/M_2(u) \rangle$, where \mathbb{V} is the affine variety introduced in Notation 13.*

From a straight-line program of length L encoding the polynomials P_j, Q_j , $1 \leq j \leq n$, the algorithm produces a straight-line program encoding M_1, M_2 . The length of the output straight-line program and the number of arithmetic operations in \mathcal{F} performed by the algorithm are linear in L and polynomial in n, d, e and $\deg \mathbb{V}$.

7 Examples

As before, let \mathcal{F} be a differential field of characteristic 0 and u a differentially transcendental element over \mathcal{F} .

Example 1. Let $\mathcal{G} = \mathcal{F}\langle u/\dot{u}, u + \dot{u} \rangle$. In this case, we have:

- $e = 1, n = 2$,
- $F_1 = \dot{u}x_1 - u, F_2 = x_2 - u - \dot{u}, q = \dot{u}$,

As the ideal $(F_1, F_2, \dot{F}_1, \dot{F}_2) = (\dot{u}x_1 - u, x_2 - u - \dot{u}, \ddot{u}x_1 + \dot{u}\dot{x}_1 - \dot{u}, \dot{x}_2 - \dot{u} - \ddot{u})$ is prime and does not contain \dot{u} , we have that $(F_1, F_2, \dot{F}_1, \dot{F}_2) : q^\infty = (F_1, F_2, \dot{F}_1, \dot{F}_2)$ and, therefore,

$$\mathbb{V} = V(F_1, F_2, \dot{F}_1, \dot{F}_2) = V(\dot{u}x_1 - u, x_2 - u - \dot{u}, \ddot{u}x_1 + \dot{u}\dot{x}_1 - \dot{u}, \dot{x}_2 - \dot{u} - \ddot{u}).$$

The dimension of \mathbb{V} equals 3. We obtain a suitable transcendence basis of the fraction field of $\mathcal{F}[x_1, x_2, \dot{x}_1, \dot{x}_2, u, \dot{u}, \ddot{u}]/(F_1, F_2, \dot{F}_1, \dot{F}_2)$ over \mathcal{F} by studying the Jacobian matrix of the polynomials:

$$\frac{\partial(F_1, F_2, \dot{F}_1, \dot{F}_2)}{\partial(x_1, x_2, \dot{x}_1, \dot{x}_2, u, \dot{u}, \ddot{u})} = \begin{pmatrix} \dot{u} & 0 & 0 & 0 & -1 & x_1 & 0 \\ 0 & 1 & 0 & 0 & -1 & -1 & 0 \\ \ddot{u} & 0 & \dot{u} & 0 & 0 & \dot{x}_1 - 1 & x_1 \\ 0 & 0 & 0 & 1 & 0 & -1 & -1 \end{pmatrix} \equiv \begin{pmatrix} \dot{u} & 0 & 0 & 0 & -1 & u/\dot{u} & 0 \\ 0 & 1 & 0 & 0 & -1 & -1 & 0 \\ \ddot{u} & 0 & \dot{u} & 0 & 0 & -\ddot{u}u/\dot{u}^2 & u/\dot{u} \\ 0 & 0 & 0 & 1 & 0 & -1 & -1 \end{pmatrix}.$$

Since the matrix obtained by removing the first three columns of this last matrix has full rank in $\mathcal{F}(u, \dot{u}, \ddot{u})$, we deduce that $\{x_1, x_2, \dot{x}_1\}$ is a transcendence basis as required.

Then, $k_0 = 0$ and so, we look for a polynomial $M(x_1, x_2, \dot{x}_1, u) \in (F_1, F_2, \dot{F}_1, \dot{F}_2)$. We compute this polynomial by an elimination procedure:

$$M(x_1, x_2, \dot{x}_1, u) = (x_1 + 1)u - x_1x_2.$$

Finally, specializing (u, \dot{u}, \ddot{u}) into $u_1 = (1, 1, 0)$ and $u_2 = (0, 1, 0)$, we compute specialization points $(1, 2, 1)$ and $(0, 1, 1)$ respectively for (x_1, x_2, \dot{x}_1) ; hence, we obtain the following Lüroth generator for \mathcal{G}/\mathcal{F} :

$$v = \frac{M_1(u)}{M_2(u)} = \frac{2u - 2}{u}.$$

In the previous example, the minimal polynomial M lies in the polynomial ideal (F_1, F_2) , that is, no differentiation of the equations is needed in order to compute it and, consequently, a Lüroth generator can be obtained as an algebraic rational function of the given generators. However, this is not always the case, as the following example shows.

Example 2. Let $\mathcal{G} = \mathcal{F}\langle \dot{u}, u + \ddot{u} \rangle$. We have:

- $e = 2, n = 2,$
- $F_1 = x_1 - \dot{u}, F_2 = x_2 - u - u^{(2)}, q = 1,$

Following our algorithmic procedure, we consider the ideal

$$(F_1, F_2, \dot{F}_1, \dot{F}_2, F_1^{(2)}, F_2^{(2)}) = (x_1 - \dot{u}, x_2 - u - u^{(2)}, \dot{x}_1 - u^{(2)}, \dot{x}_2 - \dot{u} - u^{(3)}, x_1^{(2)} - u^{(3)}, x_2^{(2)} - u^{(2)} - u^{(4)}).$$

This is a prime ideal of $\mathcal{F}[x^{[2]}, u^{[4]}]$. The variety \mathbb{V} is the zero-set of this ideal and it has dimension 5. A transcendence basis of $\mathcal{F}(\mathbb{V})$ over \mathcal{F} including a maximal subset of $x^{[2]}$ is $\{x_1, x_2, \dot{x}_1, \dot{x}_2, x_2^{(2)}\}$ and the minimal polynomial of u over $\mathcal{F}(x_1, x_2, \dot{x}_1, \dot{x}_2, x_2^{(2)})$ is

$$M = u - x_2 + \dot{x}_1.$$

Two specializations of this polynomial lead us to a Lüroth generator of \mathcal{G}/\mathcal{F} of the form $v = \frac{u+a}{u+b}$. We conclude that $\mathcal{G} = \mathcal{F}\langle u \rangle$.

References

- [1] C. Alonso, J. Gutiérrez, and T. Recio, A rational function decomposition algorithm by near-separated polynomials. *J. Symb. Comp.* 19 (1995), 527544.
- [2] P. Bürgisser, M. Clausen, M.A. Shokrollahi, *Algebraic Complexity Theory*, Grundlehren der Mathematischen Wissenschaften, vol. 315, Springer, Berlin, 1997.
- [3] G. Chèze, Nearly Optimal Algorithms for the Decomposition of Multivariate Rational Functions and the Extended Lüroth's Theorem, *J. Complexity* 26 (2010), no. 4, 344–363.
- [4] L. D'Alfonso, G. Jeronimo, G. Massaccesi, P. Solernó, On the index and the order of quasi-regular implicit systems of differential equations. *Linear Algebra and its Applications* 430 (2009), pp. 2102–2122.
- [5] L. D'Alfonso, G. Jeronimo, P. Solernó, On the complexity of the resolvent representation of some prime differential ideals. *J. Complexity* 22 (2006), no. 3, 396–430.
- [6] L. D'Alfonso, G. Jeronimo, F. Ollivier, A. Sedoglavic, P. Solernó, A geometric index reduction method for implicit systems of differential algebraic equations. *J. Symbolic Computation* 46, Issue 10 (2011), 1114–1138
- [7] J. von zur Gathen, J. Gerhard, *Modern Computer Algebra*, Cambridge University Press, NewYork, 1999.
- [8] X. Gao, T. Xu, Lüroth's theorem in differential fields, *Journal of Systems Science and Complexity* 15 (2002), no. 4, 376–383.
- [9] J. Gutiérrez, R. Rubio, D. Sevilla, On multivariate rational function decomposition. *Computer algebra (London, ON, 2001)*. *J. Symbolic Comput.* 33 (2002), no. 5, 545–562.
- [10] J. Gutiérrez, R. Rubio, D. Sevilla, Unirational Fields of Transcendence Degree One and Functional Decomposition. *Proc. of the 2001 Int. Symposium on Symb. and Alg. Comput. ISSAC'01*. ACM Press, New York (2001), 167–174.
- [11] J. Heintz, Definability and fast quantifier elimination in algebraically closed fields. *Theoret. Comput. Sci.* 24 (1983), no. 3, 239–277.
- [12] J. Heintz, T. Krick, S. Puddu, J. Sabia, A. Waissbein, Deformation techniques for efficient polynomial equation solving. *J. Complexity* 16 (2000), No. 1, 70–109.
- [13] J. Heintz, C.-P. Schnorr, Testing polynomials which are easy to compute, *Monographie 30 de l'Enseignement Mathématique*, 1982, 237254.
- [14] E.R. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, NewYork, 1973.
- [15] E.R. Kolchin, Extensions of differential fields, II. *Ann. of Math. (2)* 45 (1944), 358–361.

- [16] E.R. Kolchin, Extensions of differential fields, III. Bull. Amer. Math. Soc. 53 (1947). 397–401.
- [17] E. Kunz, Introduction to Commutative Algebra and Algebraic Geometry, Birkhäuser, Boston, MA, 1985.
- [18] J. Lüroth, Beweis eines Satzes über rationale curven, Math. Ann. , 9 (1876) pp. 163–165
- [19] G. Matera, A. Sedoglavic, Fast computation of discrete invariants associated to a differential rational mapping. J. Symbolic Comput. 36 (2003), No. 34, 473–499.
- [20] E. Netto, Über einen Lüroth gordaschen staz. Math. Ann. 46 (1895), 310–318.
- [21] F. Ollivier, Une réponse négative au problème de Lüroth différentiel en dimension 2. C.R. Acad. Sci. Paris, Serie I, t. 327, no.10, Série I, 1998, 881–886.
- [22] J.F. Ritt, Differential equations from the algebraic standpoint. Amer. Math. Soc. Colloq. Publ., Vol XIV, New York, 1932.
- [23] J.F. Ritt, Differential Algebra. Amer. Math. Soc. Colloq. Publ., Vol. 33, New York, 1950.
- [24] B. Sadik, A bound for the order of characteristic set elements of an ordinary prime differential ideal and some applications, Appl. Algebra Engrg. Comm. Comput. **10**, no. 3, (2000), 251–268.
- [25] T.W. Sederberg, Improperly parametrized rational curves, Computer Aided Geometric Design 3 (1986), 67–75.
- [26] É. Schost, Computing parametric geometric resolutions. Applicable Algebra in Engineering, Communication and Computing 13 (2003), No. 5, 349–393.
- [27] B. L. van der Waerden, Modern Algebra, Vol. I, Springer-Verlag, 1991.